METHODS, MEANS AND TECHNOLOGIES OF INFORMATION PROTECTION ON THE INTERNET

Beknazarova Saida Safibullayevna, Absamitov Bekhruz
Tashkent University of Information Technologies named after Muhammad Al- Khwarizmi, 105, A. Temur, Tashkent, 100142, Uzbekistan, saida.beknazarova@gmail.com

The data can be divided into two types:

Personal information of an individual (surname, first name, patronymic, passport data (Russian and foreign), SNILS, TIN, license numbers, data of his car, phone number, residential address, full name of the next of kin and their data, etc.);

Information of companies (legal entity: both commercial and state organizations). This includes information about the manager, employees, confidential data representing a trade secret (company turnover, bank accounts, a list of contractors - suppliers and buyers) and so on [1].

The information is stored on paper - passport, SNILS, paper copies of documents - and in electronic form on the Internet, in the programs of personnel services, in the database of telecom operators, contractors and suppliers of services, goods, etc.

Users of the information are representatives of state authorities (the Ministry of Internal Affairs, the security services, bailiffs and etc.), HR services of companies, employees of commercial organizations. The goals are very different: calling to offer your goods and services, getting acquainted with a potential employee before hiring, contact details… And among others, scammers are looking for personal and corporate data [2].

One of the main tasks of data processing and storage is to prevent unauthorized access to confidential information. This task is solved by choosing the appropriate method of protecting information on the network. In theory, all methods of protecting information on the Internet can be divided into several large groups:

- creating obstacles in the way of a threat (attack) - including restricting physical access to media;
- managing vulnerabilities and elements of the protected system;
- implementation of a set of measures, the result of which is the masking of protected information (this may include cryptographic encryption tools);
- development of an action plan, distribution of roles and access levels (regulation), in which users of an information system (IS) are required to adhere to specified protocols for using information that reduce the risks of unauthorized access to information.

Compliance with the rules of access, processing and storage of information can be achieved through coercive measures (including threats of administrative, material, criminal liability for violations) and inducement (compliance with established rules for moral, ethical and psychological reasons) [3].

The masking method is considered the only reliable way to protect information when it is transmitted over communication channels (on the Internet). The following methods also show high efficiency in corporate and local networks:

identification of users, computer network resources (through the assignment of identifiers and authentication at each session of work with data from the IP, authentication can be carried out through the use of an electronic digital signature, EDS, login-password pair and other means);

regulation of access to any resources - access control and authorization, logging of requests (requests) for example, the analysis of the correspondence of requests to the time of day (with the establishment of working time limits), the definition of restriction measures in case of unauthorized access.

Information security tools on the Internet

The means of protecting information on the Internet are:

technical and technological:

- physical - devices and systems that create obstacles in the way of intruders or destabilizing factors, including doors, locks, etc.;

- hardware - devices embedded in the IP specifically to protect information (can create obstacles or encrypt data);
- software – specialized software (software) that implements the functions of creating obstacles to the actions of intruders, encrypting data or distributing access levels;
- legislative and legal instruments, standards (at the enterprise level, these may be regulations, access rights, etc., including establishing financial liability for negligent or intentional violation of the rules for the use of IP);
- organizational, including the established practice of information processing.

Organizational methods of protecting information from its subsequent dissemination on the web include:

- restriction of published content on social networks (travel, the situation of one's home, friends' full names, birthday dates, phone numbers and other contact information);
- the use by employees of specially created and not associated with corporate accounts of personal accounts on avito.ru , youla.ru and other bulletin boards;
- control over the provision of personal information in banks, tax authorities, railway stations, air/railway ticket offices, where there may be extraneous "ears";
- control of information about employees published on the badges of line personnel is enough for the position and name (knowing the full name of the employee, it is not difficult to find his profile in social networks, i.e. uniquely identify the person);
- destruction of paper media (forms, reports) containing confidential data;
- restriction of the use of corporate accounts, email for registration and authorization in social networks, websites, and mobile applications;
- providing balanced information about employees, organizations on the website, in social networks (official pages, groups).

Information security technologies in networks

The main way to protect the transmitted data is their encryption. The strength of the cipher depends on the complexity of the algorithm used. Cryptographic (mathematical) encryption methods are protected from all types of threats, except for physical access to data carriers (with an encryption key) [1].

If the transmitted data is not secret, but only confirmation of their authenticity (authenticity of signatures) is required, then an electronic digital signature (EDS) is used. An electronic document signed by an EDS is not protected from unauthorized access; however, it cannot be changed without signaling about it.

Reference:

1. Gafner, V.V. Information security: A textbook / V.V. Gafner. - Ph/D: Phoenix, 2017— - 324 p.
2. Gromov, Yu.Yu. Information security and information protection: Textbook / Yu.Yu. Gromov, V.O. Drachev, O.G. Ivanova. - St. Oskol: TNT, 2017. - 384 p.
3. Efimova, L.L. Information security of children. Russian and foreign experience: Monograph / L.L. Efimova, S.A. Kocherga. - M.: UNITY-DANA, 2016— - 239 p.